

(12) UK Patent Application (19) GB (11) 2 333 672 (13) A

(43) Date of A Publication 28.07.1999

(21) Application No. 98016694

(22) Date of Filing 27.01.1998

(71) Applicant(s)

Stasys Limited
(Incorporated in the United Kingdom)
The Granary, 1 Waverley Lane, Farnham, Surrey,
GU9 8BB, United Kingdom

(72) Inventor(s)

Derek Ian Joseph Hopkins

(74) Agent and/or Address for Service

Fry Heath & Spence
The Old College, 53 High Street, HORLEY, Surrey,
RH6 7BN, United Kingdom

(51) INT CL⁶
H04L 12/26, G06F 17/40

(52) UK CL (Edition Q)
H&P PEUX

(56) Documents Cited

GB 2306853 A GB 2295299 A EP 0720108 A1
US 5615323 A US 5504863 A US 5270705 A
US 4907159 A

(58) Field of Search:

UK CL (Edition P) H4L LFM, H4P PEUL PEUX PEV
PPD
INT CL⁸ G06F 17/24 17/30 17/40, H04B 17/00, H04L
12/26
Online : WPI

(54) Abstract Title

Analysing tactical data link messages

(57) The application describes a method of analysing digital data-link messages comprising the steps of:

b) receiving a plurality of data link messages;

- b) assigning each data link message to one of a plurality of message groups such that each group contains data link messages of a specific message type (format);

c) within a group

(i) tabulating the messages so as to offer corresponding fields.

- (i) tabulating the messages so as
- (ii) displaying the tabulated data

(iii) displaying the tabulated data.

For each field type, it is preferred to display a list of field contents within that type, filtered to remove repeated incidence of the same content. Thus, the user is presented simultaneously with a summary of the common entries for a particular field type and any spurious or unusual entries which are highlighted. It is also useful to filter the lists to remove repeated incidence of content falling with a specified narrow range. This could be more useful for continuously variable data types such as latitude or longitude data. This is particularly applicable to tactical data link messages, e.g. between aircraft and ground stations.

Fig 2

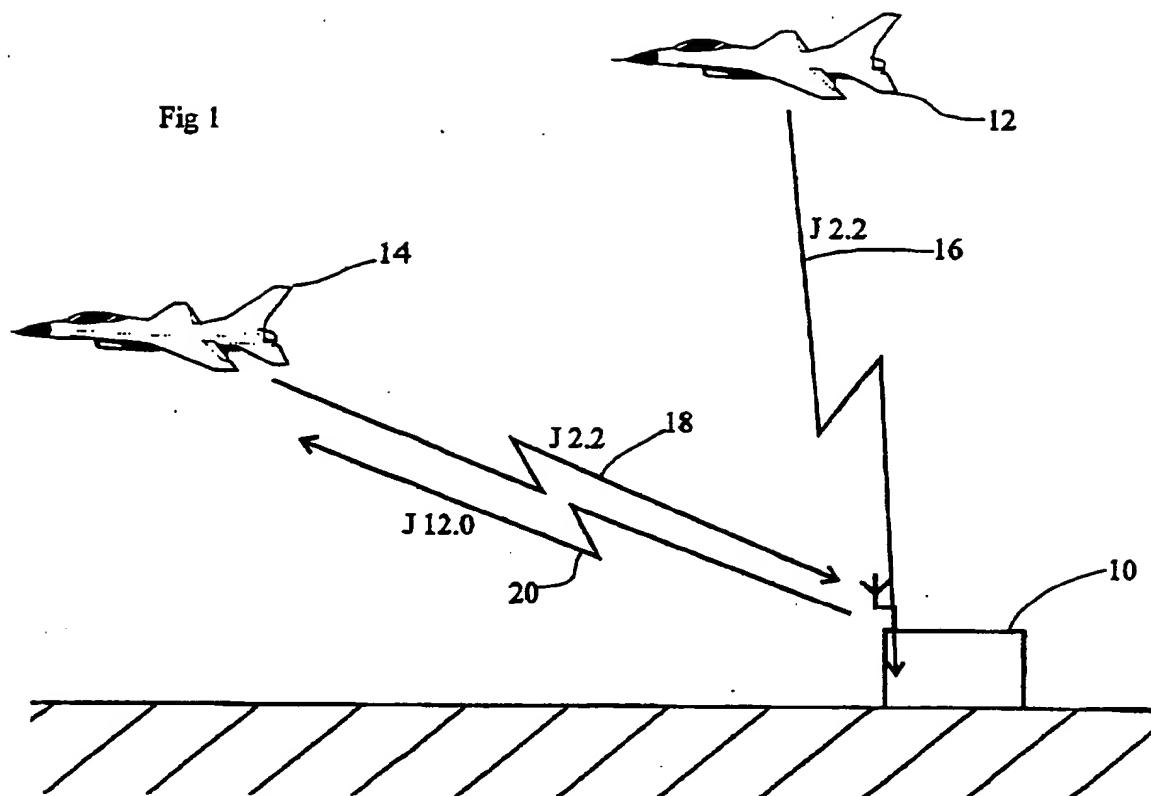


Fig 2

BEST AVAILABLE COPY

2/3

三

BEST AVAILABLE COPY

3/3

RIB 4

52.

2333672

1

ANALYSING TACTICAL DATA LINK MESSAGES

The present invention relates to a method of analysing data link messages. It is particularly useful for detecting interoperability conflicts between the various sources of such messages. In this application, the description is directed to the interpretation of tactical data link messages, but the principle of the invention can be applied to like messages.

Tactical data links operate by exchanging messages between military units such as aircraft, ships, ground stations etc, which are synchronised in a radio network. Messages are transmitted in a digital form and consist of a stream of data bits formatted according to certain rules. These rules lay down that messages have a fixed format dependent on their message type. Different message types are intended to contain different information. For example, a track message will contain position and velocity information of (for example) an aircraft, whilst a status message will contain fuel data and weapons status of the aircraft. At present, approximately fifty different types of messages are defined for each link.

The message types and formats for each type are set down according to NATO rules and in theory a platform conforming to those rules should therefore be able to communicate with any other platform which also follows those rules. In other words, the platforms are fully interoperable and can

communicate with each other satisfactorily. In practice, the rules are inevitably insufficiently comprehensive to cover every eventuality. There is therefore scope for variation between different platform implementations, and these variations typically lead to interoperability problems. For example, a receiving platform may require that an incoming message contains certain information whereas the transmitting platform for some reason does not include that information. This would result in the receiving platform discarding that message as it did not meet its processing rules.

Interoperability problems such as this can be discovered by comparing the different platform implementations with reference to their build specifications. However, the specifications themselves may be unclear and the procedure would in any case be lengthy and difficult. It is more usual for interoperability problems to be discovered during a trial when the messages are recorded and their contents matched against expected events in each platform.

The difficulty with this latter approach is that data is generated by tactical data links at a very high rate. It is normal to generate approximately 20 MB of data during a two hour flight by a single platform. This can be compressed for transmission, but for analysis will obviously need to be decompressed. A lengthy trial with a significant number of platforms will clearly generate a *prima facie* unmanageable volume of data.

It is however essential that interoperability problems are identified in order to allow their resolution. Such difficulties could significantly impair the effectiveness of armed forces in a conflict situation, the implications of which are clear.

At present, data is sorted chronologically and placed into a database. The sheer volume of data and the wide range of information that may be included within a specific message field due to the large number of message

formats means that direct inspection of the data is not physically possible on any significant scale. However, databases allow a user to present queries, which are essentially filters to select those entries which meet certain criteria. Thus, a user can present the database with queries intended to illuminate interoperability conflicts.

The use of databases to analyse the data in this way has certain defects. It is immediately apparent to a user that the databases take a significant amount of time to analyse the data and respond to the query. Whilst this could in future be solved by applying ever greater processing power to the database, it would be useful to be able to accelerate the process. At present, the various stages necessary to convert the data into a form readable by the database, enter it into the database, select appropriate queries and obtain responses and analyse those responses means that, at best, results are available several days after the trial. It would be useful if those results were available at the post-trial debrief. As this is held a matter of hours after the trial end, whilst operators memories are still fresh, this is simply not practical at present.

Existing databases also suffer from a more fundamental flaw. It is up to the user to generate queries, and therefore this requires an a priori knowledge of the type of interoperability conflicts likely to arise. The user is not generally in a position to detect unexpected interoperability errors, as the raw data cannot feasibly be inspected and the processing time required rules out the use of a large number of speculative queries aimed at detecting unlikely or unsuspected conflicts. Speculative queries also require the user to have an intimate knowledge of the type of content in particular message fields, in order to detect unusual entries. This again cannot be guaranteed, and is clearly unlikely in the case of unsuspected conflicts.

The present invention seeks to provide a more intuitive analysis method for data link messages which is capable of providing speedier

analysis.

The present invention therefore provides a method of analysing data link messages, comprising the steps of:

- a) receiving a plurality of data link messages;
- b) assigning each data link message to one of a plurality of message groups such that each group contains data link messages of a specific message type;
- c) within a group,
 - (i) tabulating the messages so as to align corresponding fields;
 - (ii) displaying the tabulated data.

The processing is preferably applied to all groups, but may be applied to a single group if it is known that this is the source of problems.

It will clearly be preferable for a group to contain all data link messages of a specific message type.

For each field type, it is preferred to display a list of field contents within that type, filtered to remove repeated incidence of the same content. Thus, the user is presented simultaneously with a summary of the common entries for a particular field type and any spurious or unusual entries. For example, if an entry normally contained a number between 1 and 12, for example, this list would comprise a random scattering of numbers in this range. If it also included a value such as 87 or a text value then at least one platform within the trial is clearly transmitting an incompatible message. It is likely that that message has a different meaning or is for some reason erroneous. This type of analysis does not require the operator to be aware a priori of the likely message content.

It is further preferred to allow the group to be filtered so as to display

only messages having a particular content for that field type, the content having been selected from the list. This enables an immediate selection to be made of erroneous or unusual entries in the list, which will then highlight the message or messages containing that entry. This would then enable the user to identify the platform or platforms generating those messages and institute appropriate corrective action.

A small modification to the above which may on occasions be useful is for the lists to remove repeated incidence of content falling with a specified narrow range. This could be more useful for continuously variable data types. It could for example be applied to latitude or longitude data to identify messages being received from platforms in an incorrect theatre.

As mentioned above, it is particularly envisaged that the invention will be applied to tactical data link messages. However, the principle can be applied to other data links and the invention is not therefore limited in this respect.

Embodiments of the present invention will now be described by way of example, with reference to the accompanying Figures, in which:

Figure 1 shows the exchange of tactical data link messages;

Figure 2 shows the tactical data link messages arranged and displayed according to the present invention;

Figure 3 shows an arrangement similar to Figure 2 employing a commercially available programme; and

Figure 4 shows the data of Figure 3 being analysed.

Tactical data links operate by exchanging messages between units

(aircrafts, ships, ground stations) which are synchronised in a radio network. Several different links are implemented, and are known as Link x where x is a number, Link 11, Link 16 etc. The different links use different radio signals and different radio sets to transmit and receive information. The messages are transmitted in digital form, consisting of a stream of data bits formatted according to rules set out in the Link standard. For Links such as Link 16, the messages are transmitted at a high rate and contain information accurate to within a few seconds.

The messages are formatted as different types, each type having a fixed format and containing similar information. The different message types have completely different formats and contain different information. For example, the types may consist of a track message, which contains position and velocity of a track, and a status message which contains fuel and weapons status of an aircraft. Within the framework of Link 16, some 50 different types of message are defined.

Within the structure of Link 16, each platform is assigned time slots of 7.8 ms duration and transmits messages only in those slots (but not necessarily in all of them). Messages may be transmitted regularly at defined intervals, or as "one offs" resulting from some operator action. Messages can be one of about 50 different types, which correspond to different possibilities for information exchange. For Link 16, each message type has a unique designation as a two part number of the form x,y. Thus, there are 256 different designations possible, of which approximately 50 are used, as mentioned above. Each message may contain between about 50 and 300 bits of information. The message is split into a number of fields which contain information relevant to the use of that particular message. For example, a track message will contain fields for latitude, longitude, speed, aircraft type etc. The representation of each field is fixed for a particular message type, so that a message can be decoded if the structure is known and the message type received. Some examples of messages are

given below.

Number	Name	Use
J0.0	Initial Entry	Allows units to synchronise to the network
J2.2	Air PPLI	Transmitted by Link 16 equipped units to give precise positional and identification data
J3.2	Air Track	Transmitted by command and control units to disseminate track data on the network
J12.0	Mission Assignment	One-off message used to assign a tactical mission to a controlled unit
J13.0	Airfield Status	Gives weather and other information about airfields

By way of example, the list of fields for an Air PPLI message includes latitude, longitude, course, speed, height, relay status, airborne status, voice call sign and platform type.

All tactical data links and certain other types of data link such as buses that connect processors in some data processing systems have a similar message structure.

A recording of a tactical data link will contain all messages that have been transmitted by all units with a certain time frame. The recording contains message of different types, ordered chronologically. The analysis tool must decode messages into fields and sort them. In the past, using text-based analysis tools, the messages have been sorted chronologically.

Figure 1 illustrates tactical data links in progress, transferring messages 16, 18, 20 to and from a ground station 10 and operating aircraft 12, 14.

Figure 2 shows the manner in which data is ordered and structured

according to the present invention. Thus, messages are first sorted by message type and grouped accordingly. Within a message group, they can be sorted chronologically if desired. The messages are then tabulated such that each field is displayed in an aligned relationship to other fields.

Figure 3 shows the same data displayed by a commercially available programme, Microsoft Excel. Microsoft is a registered Trade Mark. Markers 50 indicate that a drop down menu can be selected, as shown in Figure 4, to reveal all the discrete values within that field. Anomalous values such as that illustrated at 52 are clearly highlighted. Selection of these values from the field results in the programme automatically applying a filter aimed at selecting that or those messages. These messages can then be inspected individually to trace the source platform.

It will be apparent that use of the analysis method set out above enables unusual or spurious entries to be detected very quickly. Messages such as the Air PPLI type include a total of forty fields, so it will therefore take only a matter of seconds to look through the individual filter results and identify spurious or unusual entries. The tabulated storage method is also very much less unwieldy than a database, and therefore can be filtered to reveal the erroneous message much more quickly. In tests, analysis results have been available in time for the post-exercise debrief, a matter of hours. This compares with the several days required to analyse the same data through the use of a database.

It will be appreciated that many variations could be made to the above described example without departing from the scope of the present invention.

CLAIMS:

1. A method of analysing data link messages, comprising the steps of:
 - a) receiving a plurality of data link messages;
 - b) assigning each data link message to one of a plurality of message groups such that each group contains data link messages of a specific message type;
 - c) within a group,
 - (i) tabulating the messages so as to align corresponding fields;
 - (ii) displaying the tabulated data.
2. A method according to claim 1 wherein the processing is applied to all groups.
3. A method according to claim 1 or claim 2 wherein each group contains all data link messages of a specific message type.
4. A method according to any preceding claim wherein a list of field contents is displayable for each field type, filtered to remove repeated incidence of the same content.
5. A method according to claim 4 wherein the list is sorted.
6. A method according to claim 4 or claim 5 wherein the group is filtered so as to display only messages having a particular content for that field type, the content having been selected from the list.
7. A method according to any one of claims 4 to 6 wherein the lists are filtered to remove repeated incidence of content falling with a specified range.

8. A method according to any preceding claim in which the data link messages are tactical data link messages.
9. A method of analysing data link messages substantially as herein described with reference to and/or as illustrated in the accompanying figures.



The
Patent
Office
11



INVESTOR IN PEOPLE

Application No: GB 9801669.4
Claims searched: 1-9

Examiner: Keith Williams
Date of search: 22 December 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK CI (Ed.P): H4P (PEUL, PEUX, PEV, PPD); H4L (LFM)

Int CI (Ed.6): H04L 12/26; H04B 17/00; G06F 17/24, 17/30, 17/40

Other: Online WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	GB 2306863 A Fujitsu - see abstract (& US 5740355)	1-3
A	GB 2295299 A Enterprise Network Services Inc. - see abstract	1
X	EP 0720108 A1 Aegis Star Corp. - see page 3, column 2, lines 9-15; abstract	1-3
X	US 5615323 Concord Communications Inc. - see abstract	1
A	US 5504863 Fujitsu - see abstract	1
X	US 5270705 US Navy - see eg columns 4 and 5	1-3
X	US 4907159 US Philips - see abstract (& EP 0290679)	1-3

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.